UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/761,920	01/20/2004	Vincent Piel	500110459-2	4097

22879 7590 04/25/2011

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528

EXAMINER	
PATEL, NIRAV B	
ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
04/25/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
ipa.mail@hp.com
laura.m.clark@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte VINCENT PIEL

Appeal 2009-006975
Application 10/761,920
Technology Center 2400

Before JAY P. LUCAS, STEPHEN C. SIU, and DEBRA K. STEPHENS, *Administrative Patent Judges*.

SIU, *Administrative Patent Judge.*

DECISION ON APPEAL

This is an appeal under 35 U.S.C. § 134(a) from the Examiner's final rejection of claims 1-17. We have jurisdiction under 35 U.S.C. § 6(b).

We reverse.

STATEMENT OF THE CASE

The invention relates to the prevention or deterrence of the theft of computers and computer components (Spec. 1, ll. 3-5). One aspect of the invention is the performance of a security check when a computer is detected to have been in an unpowered state, instead of performing the security check even when the computer is booting from a "soft-off" operating state (Spec. 4, ll. 23-30).

Independent claim 1 is illustrative:

> 1. A component for a computer, the component comprising a firmware element operable to perform a security check to verify the computer is connected to an authorised network, the security check comprising the steps of:
>
> generating a random number,
>
> encrypting the random number with a public key of a public/private key pair associated with the network,
>
> transmitting the encrypted random number to a network device via the network,
>
> receiving a response comprising a number from the network device, and
>
> permitting operation of at least a subsystem of the computer if the response is in accordance with the random number,
>
> the step of permitting operation of at least a subsystem of the computer if the response is in accordance with the random number comprises comparing the random

> number transmitted to the network device with the number in the response and permitting operation if the number in the response matches the random number transmitted to the network device, wherein the security check is performed when the computer is detected to have been in an unpowered state since a previous security check.

(Claims Appx, App. Br. 25).

The Examiner relies on the following references as evidence in support of the rejection:

Herzi	US 6,484,262 B1	Nov. 19, 2002
Hamamoto	US 2002/0000913 A1	Jan. 3, 2002

The Examiner rejected the claims as follows:

Claims 1-17 under 35 U.S.C. § 103(a) as being unpatentable over Herzi and Hamamoto.

ISSUE

With regard to the obviousness rejection of claims 1-17, Appellant submits that "*Herzi* describes that a security measure is implemented 'upon every boot of the particular computer system,' at regular intervals of time, or 'any duration of time as may be established for a given security policy'" (App. Br. 10). Appellant further submits that "*Hamamoto* describes a monitoring device for an automatic teller machine, where a backup power supply is put in use for the monitoring device when the automatic teller machine is powered off" (*id.*).

Therefore, we identify the following issue:

Did the Examiner err in finding that Herzi and Hamamoto would have taught or suggested performing a security check when the computer is detected to have been in an unpowered state since a previous security check?

FINDINGS OF FACT

The following Findings of Fact (FF) are shown by a preponderance of the evidence.

1. Herzi discloses "authentication upon every boot of [a] particular computer system" (col. 4, ll. 6-7). Herzi also discloses that obtaining authorization on every boot is unnecessary if "the computer system incorporate[s] the security measure . . . during a specified time period, or security check interval" (col. 4, ll. 7-16). A "time period or security check interval may include a daily interval, weekly interval, monthly interval or any other duration of time" (col. 4, ll. 16-18).

2. Hamamoto discloses a "monitoring device [that] comprises . . . means operative when the automatic teller machine is powered off . . . for supplying the security monitoring controller with the power from a backup power supply unit . . . so that the security monitoring unit can be continued even if the automatic teller machine is powered off" (¶ [0006]). The security monitoring unit monitors "a situation by means of a video camera and a microphone when vibrations, heat or the like is sensed" (¶ [0017]).

PRINCIPLES OF LAW

The question of obviousness is resolved on the basis of underlying factual determinations including (1) the scope and content of the prior art,

(2) any differences between the claimed subject matter and the prior art, and (3) the level of skill in the art. *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 17-18 (1966).

ANALYSIS

Obviousness rejection of claims 1-17

Appellant challenges the Examiner's finding that Herzi and Hamamoto would have taught or suggested the limitation of performing a security check when it is detected that a computer was been unpowered since the previous security check. We agree that the Examiner erred.

Herzi teaches performing a security check every time a system boots, during specified time periods, or at regular intervals (FF 1). Accordingly, Herzi's disclosure is limited to performing a security check based on booting—regardless of whether the boot was caused by an unpowered state—or based on time. These teachings do not include detection that the system was in an unpowered state. By itself, Herzi does not teach or suggest performing a security check when an unpowered state has been detected.

The Examiner instead relies on Hamamoto as teaching or suggesting that "the security check is performed when the computer is detected to have been in an unpowered state since a previous security check" (Ans. 4). However, Hamamoto merely teaches that a backup power supply enables a security monitoring unit to continue even if the monitored machine is powered off (FF 2). This teaches or suggests detecting that power must be drawn from an alternative source because power is currently unavailable. But detecting that power is currently unavailable is not the same as detecting that a system had been in an unpowered state.

Furthermore, Hamamoto's security monitoring unit obtains video and audio data "when vibrations, heat, or the like is sensed" (FF 2). Neither the data collected nor the conditions listed include detection that the system had been in an unpowered state. Because Hamamoto does not teach or suggest detecting that a system had been in an unpowered state, we conclude that Hamamoto does not cure the deficiencies of Herzi.

For at least these reasons, we find the Examiner erred in rejecting claims 1-17.

CONCLUSIONS OF LAW

Based on the findings of fact and analysis above, we find the Examiner erred in finding that Herzi and Hamamoto would have taught or suggested performing a security check when the computer is detected to have been in an unpowered state since a previous security check.

DECISION

We reverse the Examiner's decision rejecting claims 1-17 under 35 U.S.C. § 103(a).

REVERSED